Math 332 Winter 2023, Lecture 11: Rings

website: `https://www.cip.ifi.lmu.de/~grinberg/t/23wa`

1. Rings and ideals (cont'd)

1.9. Quotient rings (cont'd)

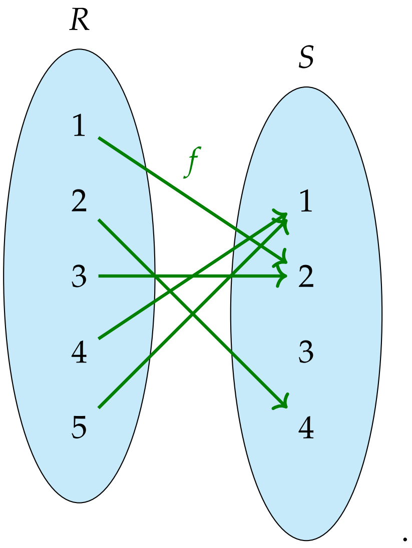
1.9.7. The First Isomorphism Theorem for sets

We begin with some basic set theory.

Consider a map $f : R \to S$ from some set R to some set S. Then, I claim that there is a bijection[1] hiding inside f.

What do I mean by this?

For an example, let $R = \{1, 2, 3, 4, 5\}$ and $S = \{1, 2, 3, 4\}$, and let $f : R \to S$ be the map that sends $1, 2, 3, 4, 5$ to $2, 4, 2, 1, 1$, respectively. Here is an illustration of this map using a standard "blobs and arrows" diagram:



As you see, this map f is neither injective nor surjective, thus certainly not bijective. However, I claim that I can **make** it bijective, by appropriately tweaking its domain R and its target S as well as the map f itself. Namely:

- First, I make f surjective. To do so, I replace the target S by the image $f(R) = \{f(r) \mid r \in R\}$ of the map f. This way, I throw away all elements

[1] "Bijection" means the same as "bijective map" (i.e., a map that is both injective and surjective) and as "1-to-1 correspondence". Also, it is worth recalling that a map is bijective if and only if it is invertible (i.e., has an inverse).

of S that are not taken as values by the map f. The resulting map

$$\begin{aligned} \widetilde{f} : R &\to f(R), \\ r &\mapsto f(r) \end{aligned}$$

(which differs from f only in its choice of target) is thus surjective.

- Next, I make f (or, more precisely, $\widetilde{f}$) injective. To do so, I equate every pair of elements $a, b \in R$ that satisfy $f(a) = f(b)$. The rigorous way to do so is to replace the elements of R by their equivalence classes with respect to an appropriately chosen equivalence relation. To wit: We define a binary relation $\sim$ on the set R by stipulating that two elements $a, b \in R$ should satisfy $a \sim b$ if and only if $f(a) = f(b)$. This relation $\sim$ is an equivalence relation[2], and will be called **f-equivalence**. Its equivalence classes will be called **f-classes**, and we will use the notation $\overline{r}$ for the f-class that contains a given element $r \in R$. We let R/f denote the set of all f-classes.

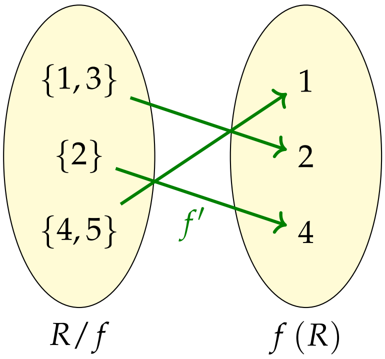
  Now, consider the map

  $$\begin{aligned} f' : R/f &\to f(R), \\ \overline{r} &\mapsto f(r), \end{aligned}$$

  which sends each f-class $\overline{r}$ to the value $f(r)$. This map f' is well-defined, since $f(r)$ depends not on the element r but only on its f-class $\overline{r}$ (because if two elements $a, b \in R/f$ have the same f-class, then $a \sim b$ and thus $f(a) = f(b)$ by the very definition of f).

  Just like $\widetilde{f}$, the map f' is surjective (since every element of its target $f(R)$ is taken as a value by f, and thus also by f'). But f' is also injective, since any two elements a, b of R that satisfy $f(a) = f(b)$ have already been merged into the same f-class in R/f. Thus, f' is both injective and surjective, hence bijective.

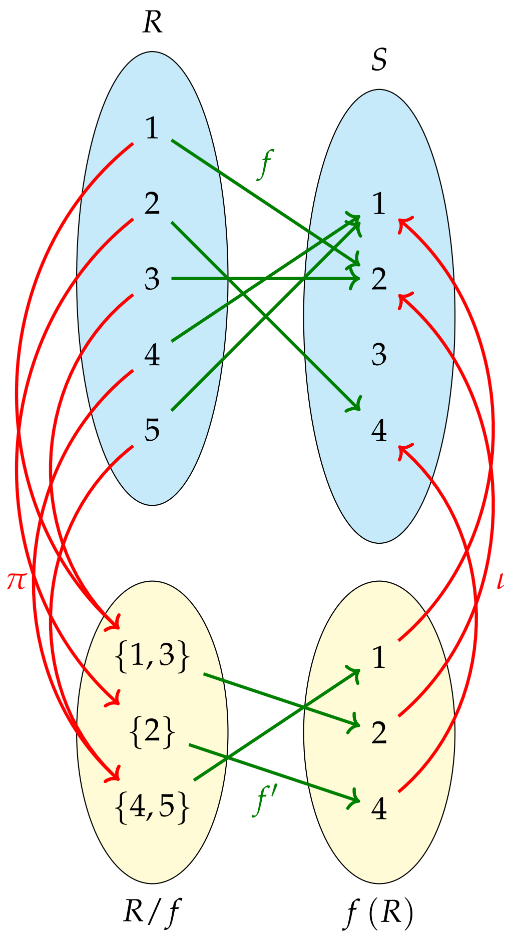
We might call f' the **bijectivization** of f (although I don't think there is a standard name for f'). In our above example, this map f' looks as follows:



.

[2] For example, it is transitive because if three elements $a, b, c \in R$ satisfy $f(a) = f(b)$ and $f(b) = f(c)$, then $f(a) = f(b)$.

Moreover, the maps f and f' fit together into a nice picture with two other rather natural maps:



Here, $\pi : R \to R/f$ is the **canonical projection** (i.e., the map that sends each $r \in R$ to its f-class $\overline{r}$), and $\iota : f(R) \to S$ is the **canonical inclusion** (i.e., the map that sends each $s \in f(R)$ to s). These four maps f, f', π, ι satisfy

$$f = \iota \circ f' \circ \pi,$$

which means (in the language of §1.9.5) that the diagram

$$\begin{tikzcd}
R \arrow[r, "f"] \arrow[d, "\pi"'] & S \\
R/f \arrow[r, "f'"'] & f(R) \arrow[u, "\iota"']
\end{tikzcd}$$

is commutative.

For the sake of completeness, let us state this all as a theorem:

Theorem 1.9.9 (First Isomorphism Theorem for sets)**.** Let R and S be any two sets, and let $f : R \to S$ be any map.

Let $\sim$ be the binary relation on the set R defined by requiring that two elements $a, b \in R$ satisfy $a \sim b$ if and only if $f(a) = f(b)$.

(a) This relation $\sim$ is an equivalence relation.

Let us refer to this relation $\sim$ as **f-equivalence**, and let us refer to its equivalence classes as the **f-classes**. Let R/f denote the set of all f-classes. For any $r \in R$, we let $\overline{r}$ denote the f-class that contains r.

(b) The image $f(R) := \{f(r) \mid r \in R\}$ of f is a subset of S.

(c) The map

$$\begin{aligned} f' : R/f &\to f(R), \\ \overline{r} &\mapsto f(r) \end{aligned}$$

is well-defined and bijective.

(d) Let $\pi : R \to R/f$ denote the **canonical projection** (i.e., the map that sends each $r \in R$ to its f-class $\overline{r}$). Let $\iota : f(R) \to S$ denote the **canonical inclusion** (i.e., the map that sends each $s \in f(R)$ to s). Then, the map f' defined in part **(c)** satisfies

$$f = \iota \circ f' \circ \pi.$$

In other words, the diagram

$$\begin{tikzcd} R \arrow[r, "f"] \arrow[d, "\pi"'] & S \\ R/f \arrow[r, "f'"'] & f(R) \arrow[u, "\iota"'] \end{tikzcd} \qquad (1)$$

is commutative.

Proof. Part **(b)** is obvious. We explained the proofs of parts **(a)** and **(c)** before even stating this theorem. It remains to prove part **(d)**.

(d) For each $r \in R$, we have

$$\begin{aligned} \left(\iota \circ f' \circ \pi\right)(r) &= \iota\left(f'(\pi(r))\right) \\ &= f'(\pi(r)) \qquad \text{(since the definition of } \iota \text{ yields } \iota(s) = s \text{ for each } s \in S) \\ &= f'(\overline{r}) \qquad \text{(since the definition of } \pi \text{ yields } \pi(r) = \overline{r}) \\ &= f(r) \qquad \left(\text{by the definition of } f'\right). \end{aligned}$$

In other words, $\iota \circ f' \circ \pi = f$. Thus, $f = \iota \circ f' \circ \pi$. In other words, the diagram (1) is commutative. This proves Theorem 1.9.9 **(d)**. □

1.9.8. The First Isomorphism Theorem for rings

Now, let us extend the First Isomorphism Theorem to rings and ring morphisms instead of arbitrary sets and maps.

Theorem 1.9.10 (First Isomorphism Theorem for rings, elementwise form)**.** Let R and S be two rings, and let $f : R \to S$ be a ring morphism. Then:

(a) The kernel $\operatorname{Ker} f$ is an ideal of R. Thus, $R/\operatorname{Ker} f$ is a quotient ring of R. As a set, $R/\operatorname{Ker} f$ is precisely the set R/f defined in Theorem 1.9.9. The f-classes (as defined in Theorem 1.9.9) are precisely the cosets of $\operatorname{Ker} f$.

(b) The image $f(R) := \{f(r) \mid r \in R\}$ of f is a subring of S.

(c) The map

$$\begin{aligned} f' : R/\operatorname{Ker} f &\to f(R), \\ \overline{r} &\mapsto f(r) \end{aligned}$$

is well-defined and is a ring isomorphism.

(d) This map f' is precisely the map f' defined in Theorem 1.9.9 **(c)**.

(e) Let $\pi : R \to R/\operatorname{Ker} f$ denote the **canonical projection** (i.e., the map that sends each $r \in R$ to its f-class $\overline{r}$). Let $\iota : f(R) \to S$ denote the **canonical inclusion** (i.e., the map that sends each $s \in f(R)$ to s). Then, the map f' defined in part **(c)** satisfies

$$f = \iota \circ f' \circ \pi.$$

In other words, the diagram

$$\begin{tikzcd} R \arrow[r, "f"] \arrow[d, "\pi"'] & S \\ R/f \arrow[r, "f'"'] & f(R) \arrow[u, "\iota"'] \end{tikzcd}$$

is commutative.

(f) We have $R/\operatorname{Ker} f \cong f(R)$ as rings.

Proof. **(a)** We know that $\operatorname{Ker} f$ is an ideal of R (by Theorem 1.8.4 in Lecture 7), and therefore $R/\operatorname{Ker} f$ is a quotient ring of R.

Let us next prove that the f-classes (as defined in Theorem 1.9.9) are precisely the cosets of $\operatorname{Ker} f$.

Indeed, let $\sim$ be the equivalence relation on R defined in Theorem 1.9.9. Then, the f-classes are defined as the equivalence classes of this relation $\sim$. For any $a, b \in R$, we have $f(b) - f(a) = f(b - a)$ (since f is a ring morphism and thus respects differences). For any two elements $a, b \in R$, we have the chain of equivalences

$$\begin{aligned}
& (a \sim b) \\
\Longleftrightarrow\ & (f(a) = f(b)) && \text{(by the definition of } \sim\text{)} \\
\Longleftrightarrow\ & (f(b) - f(a) = 0) \\
\Longleftrightarrow\ & (f(b-a) = 0) && \text{(since } f(b) - f(a) = f(b-a)\text{)} \\
\Longleftrightarrow\ & (b - a \in \operatorname{Ker} f) && \text{(by the definition of } \operatorname{Ker} f\text{)} .
\end{aligned}$$

However, if $a \in R$ is arbitrary, then

$$\begin{aligned}
& (\text{the } f\text{-class that contains } a) \\
& = (\text{the equivalence class of the relation } \sim \text{ that contains } a) \\
& \qquad\qquad (\text{since the } f\text{-classes are the equivalence classes of } \sim) \\
& = \{ b \in R \mid a \sim b \} \qquad (\text{by the definition of equivalence classes}) \\
& = \{ b \in R \mid b - a \in \operatorname{Ker} f \} \\
& \qquad\qquad \left(\begin{array}{c} \text{by the equivalence } (a \sim b) \Longleftrightarrow (a - b \in \operatorname{Ker} f) \\ \text{that we proved above} \end{array} \right) \\
& = \{ b \in R \mid b \in a + \operatorname{Ker} f \} \\
& = a + \operatorname{Ker} f \\
& = (\text{the coset of } \operatorname{Ker} f \text{ that contains } a)
\end{aligned}$$

(since the coset of $\operatorname{Ker} f$ that contains a is $a + \operatorname{Ker} f$ by definition). Thus, the f-classes are precisely the cosets of $\operatorname{Ker} f$.

In other words, the cosets of $\operatorname{Ker} f$ are precisely the f-classes. Hence, the set $R/\operatorname{Ker} f$ is precisely the set R/f (since the former set consists of the cosets of $\operatorname{Ker} f$, while the latter set consists of the f-classes). This concludes the proof of Theorem 1.9.10 **(a)**.

(b) This is just Proposition 1.7.5 in Lecture 6.

(c) Theorem 1.9.10 **(a)** yields that $R/f = R/\operatorname{Ker} f$, and that the f-classes are precisely the cosets of $\operatorname{Ker} f$. Hence, the meaning of the notation $\overline{r}$ in Theorem 1.9.9 is identical with the meaning of this notation in Theorem 1.9.10 (indeed, the former denotes the f-class that contains r, whereas the latter denotes the coset of $\operatorname{Ker} f$ that contains r; but as we just said, the f-classes are precisely the cosets of $\operatorname{Ker} f$). Hence, Theorem 1.9.9 **(c)** shows that the map

$$\begin{aligned}
f' : R/f &\to f(R), \\
\overline{r} &\mapsto f(r)
\end{aligned}$$

is well-defined and bijective. Since $R/f = R/\operatorname{Ker} f$ (as sets), we can restate this as follows: The map

$$\begin{aligned}
f' : R/f &\to f(R), \\
\overline{r} &\mapsto f(r)
\end{aligned}$$

is well-defined and bijective. It remains to prove that this map f' is a ring isomorphism.

We shall first show that f' is a ring morphism. Indeed, this is a direct consequence of Theorem 1.9.6 from Lecture 10 (applied to $I = \operatorname{Ker} f$), since we have $f(\operatorname{Ker} f) = 0$ (by the definition of $\operatorname{Ker} f$). Alternatively, we can prove this by hand[3]. Hence, f' is an invertible ring morphism (invertible because it is bijective). Thus, f' is a ring isomorphism (since Proposition 1.7.6 from Lecture 6 shows that any invertible ring morphism is a ring isomorphism). Thus, the proof of Theorem 1.9.10 **(c)** is finished.

(d) As we have seen in our above proof of Theorem 1.9.10 **(c)**, we have $R/f = R/\operatorname{Ker} f$, and the meaning of the notation $\overline{r}$ in Theorem 1.9.9 is identical with the meaning of this notation in Theorem 1.9.10. Thus, the map f' in Theorem 1.9.10 **(c)** is precisely the map f' defined in Theorem 1.9.9 **(c)**. This proves Theorem 1.9.10 **(d)**.

(e) As we have seen in our above proof of Theorem 1.9.10 **(c)**, we have $R/f = R/\operatorname{Ker} f$, and the meaning of the notation $\overline{r}$ in Theorem 1.9.9 is identical with the meaning of this notation in Theorem 1.9.10. Therefore, the maps π and ι defined in Theorem 1.9.10 **(e)** are precisely the maps π and ι in Theorem 1.9.9 **(e)**. Hence, the claim of Theorem 1.9.10 **(e)** follows immediately from Theorem 1.9.9 **(e)**.

(f) This follows directly from Theorem 1.9.9 **(c)**. □

As our proof has shown, Theorem 1.9.9 **(c)** is merely a partial improvement on the universal property of quotient rings (Theorem 1.9.6 in Lecture 10): The latter yields a ring morphism, while the former produces a ring **iso**morphism

[3] *Proof.* We must show that f' is a ring morphism, i.e., that f' respects addition, multiplication, zero and unity.

To see that f' respects multiplication, we must show that $f'(xy) = f'(x) \cdot f'(y)$ for any $x, y \in R/\operatorname{Ker} f$. So let $x, y \in R/\operatorname{Ker} f$ be arbitrary. Then, we can write x and y as $x = \overline{a}$ and $y = \overline{b}$ for two elements $a, b \in R$. Consider these a, b. From $x = \overline{a}$ and $y = \overline{b}$, we obtain $xy = \overline{a} \cdot \overline{b} = \overline{ab}$ (by the definition of the product on $R/\operatorname{Ker} f$), so that

$$\begin{aligned} f'(xy) &= f'\left(\overline{ab}\right) = f(ab) && \text{(by the definition of } f'\text{)} \\ &= f(a) \cdot f(b) && \text{(since } f \text{ is a ring morphism)}. \end{aligned}$$

Comparing this with

$$f'\left(\underbrace{x}_{=\overline{a}}\right) \cdot f'\left(\underbrace{y}_{=\overline{b}}\right) = \underbrace{f'(\overline{a})}_{\substack{=f(a) \\ \text{(by the} \\ \text{definition of } f'\text{)}}} \cdot \underbrace{f'\left(\overline{b}\right)}_{\substack{=f(b) \\ \text{(by the} \\ \text{definition of } f'\text{)}}} = f(a) \cdot f(b),$$

we obtain $f'(xy) = f'(x) \cdot f'(y)$, just as desired. Thus, we have shown that f' respects multiplication. Similarly, f' satisfies all the other axioms in the definition of a ring morphism.

(but in a less general setup: $R/\operatorname{Ker} f$ instead of R/I). Nevertheless, it is a useful result, as it can be used to identify certain quotient rings as (isomorphic copies of) known rings.

Here are some examples for what can be done with the first isomorphism theorem:

- Consider the map

$$f : \mathbb{Q}^{4\leq 4} \to \mathbb{Q}^{2\leq 2},$$
$$\begin{pmatrix} a & b & c & d \\ 0 & u & v & w \\ 0 & 0 & x & y \\ 0 & 0 & 0 & z \end{pmatrix} \mapsto \begin{pmatrix} u & v \\ 0 & x \end{pmatrix},$$

  which removes the "outer shell" (i.e., the first and the fourth rows and columns) from an upper-triangular 4×4-matrix. This map f is a ring morphism[4]. The kernel of this morphism f is

$$\begin{aligned}
\operatorname{Ker} f &= \left\{ \begin{pmatrix} a & b & c & d \\ 0 & u & v & w \\ 0 & 0 & x & y \\ 0 & 0 & 0 & z \end{pmatrix} \in \mathbb{Q}^{4\leq 4} \mid \begin{pmatrix} u & v \\ 0 & x \end{pmatrix} = 0 \right\} \\
&= \left\{ \begin{pmatrix} a & b & c & d \\ 0 & u & v & w \\ 0 & 0 & x & y \\ 0 & 0 & 0 & z \end{pmatrix} \in \mathbb{Q}^{4\leq 4} \mid u = v = x = 0 \right\} \\
&= \left\{ \begin{pmatrix} a & b & c & d \\ 0 & 0 & 0 & w \\ 0 & 0 & 0 & y \\ 0 & 0 & 0 & z \end{pmatrix} \in \mathbb{Q}^{4\leq 4} \right\}.
\end{aligned}$$

So you can conclude right away that $\operatorname{Ker} f$ is an ideal of $\mathbb{Q}^{4\leq 4}$. Moreover, the image $f\left(\mathbb{Q}^{4\leq 4}\right)$ is the whole $\mathbb{Q}^{2\leq 2}$ (that is, the map f is surjective). The First Isomorphism theorem (Theorem 1.9.10 **(c)**) yields a ring isomorphism

$$\begin{aligned}
f' : \mathbb{Q}^{4\leq 4} / \operatorname{Ker} f &\to f\left(\mathbb{Q}^{4\leq 4}\right), \\
\overline{r} &\mapsto f(r).
\end{aligned}$$

[4] Proving this is a nice exercise in matrix multiplication! It is obvious that f respects addition, zero and unity, but you might be skeptical that it respects multiplication. (And indeed, the analogous map

$$F : \mathbb{Q}^{4\times 4} \to \mathbb{Q}^{2\times 2},$$
$$\begin{pmatrix} a & b & c & d \\ a' & b' & c' & d' \\ a'' & b'' & c'' & d'' \\ a''' & b''' & c''' & d''' \end{pmatrix} \mapsto \begin{pmatrix} b' & c' \\ b'' & c'' \end{pmatrix},$$

which removes the "outer shell" from an arbitrary (not upper-triangular) 4×4-matrix, does not respect multiplication.) You can convince yourself of this property of f by a straightforward computation:

$$\begin{pmatrix} a & b & c & d \\ 0 & u & v & w \\ 0 & 0 & x & y \\ 0 & 0 & 0 & z \end{pmatrix} \begin{pmatrix} a' & b' & c' & d' \\ 0 & u' & v' & w' \\ 0 & 0 & x' & y' \\ 0 & 0 & 0 & z' \end{pmatrix} = \begin{pmatrix} aa' & ab' + bu' & ac' + bv' + cx' & ad' + bw' + cy' + dz' \\ 0 & uu' & uv' + vx' & uw' + vy' + wz' \\ 0 & 0 & xx' & xy' + yz' \\ 0 & 0 & 0 & zz' \end{pmatrix}$$

(note the uu', $uv' + vx'$, 0 and xx' entries, which are precisely the entries of $\begin{pmatrix} u & v \\ 0 & x \end{pmatrix} \begin{pmatrix} u' & v' \\ 0 & x' \end{pmatrix}$).

In other words, it yields a ring isomorphism

$$\begin{aligned} f' : \mathbb{Q}^{4\leq 4} / \operatorname{Ker} f &\to \mathbb{Q}^{2\leq 2}, \\ \overline{\begin{pmatrix} a & b & c & d \\ 0 & u & v & w \\ 0 & 0 & x & y \\ 0 & 0 & 0 & z \end{pmatrix}} &\mapsto \begin{pmatrix} u & v \\ 0 & x \end{pmatrix} \end{aligned}$$

(since $f\left(\mathbb{Q}^{4\leq 4}\right) = \mathbb{Q}^{2\leq 2}$). In particular, $\mathbb{Q}^{4\leq 4} / \operatorname{Ker} f \cong \mathbb{Q}^{2\leq 2}$.

- We have not properly defined polynomials yet, but once we will, you will be inundated with good examples for the First Isomorphism Theorem. Many of these examples will have the form

  $$(\text{a polynomial ring}) \,/\, (\text{an ideal}) \cong (\text{a ring of numbers})\,.$$

  For instance, recalling that $\mathbb{R}[x]$ is the ring of all polynomials in one indeterminate x with real coefficients, we have a ring morphism

  $$\begin{aligned} f : \mathbb{R}[x] &\to \mathbb{C}, \\ p &\mapsto p(i) \end{aligned}$$

  (which sends each polynomial $p \in \mathbb{R}[x]$ to its value at the imaginary unit $i = \sqrt{-1}$). This morphism is surjective (that is, $f(\mathbb{R}[x]) = \mathbb{C}$) and has kernel $\operatorname{Ker} f = \left(x^2+1\right)\mathbb{R}[x]$ (the principal ideal generated by x^2+1), so that the First Isomorphism theorem (Theorem 1.9.10 **(f)**) yields

  $$\mathbb{R}[x] \,/\, \left(\left(x^2+1\right)\mathbb{R}[x]\right) \cong \mathbb{C}.$$

  Informally, this is saying that if you are working with polynomials in an indeterminate x over $\mathbb{R}$, but you equate the polynomial x^2+1 to zero (that is, you pretend that $x^2 = -1$), then you obtain the complex numbers. This is the rigorous concept behind the classical idea that "the complex numbers are what you get if you start with the real numbers and adjoin a root of the polynomial x^2+1". We will make this precise in a later chapter.